

Press release

Date: 24 February 2011

For immediate release

Name: Geert Decorte

Title: Press & Public Relations Barco Silex

Tel: +32 10 454904

Email: geert.decorte@barco.com

Barco Silex presents enhanced version of Public Key hardware solution

Louvain-la-Neuve, Belgium – February 24, 2011 – Barco Silex, Barco's center of competence for electronic design, has announced an enhanced version of its Public Key Hardware Accelerator. The BA414E is the first member of a new generation of Crypto Intellectual Property (IP) cores developed, validated and licensed by Barco Silex.

Capitalizing on its silicon-proven experience with cryptography and security hardware processing, Barco Silex is sharing its strong expertise in ASIC, System-on-Chip & FPGA design and its experience as IP Integrator & Developer by offering innovative & cost-efficient solutions for Embedded Security.

"The BA414E Public Key Crypto Engine is the first product of a new family of Cryptography and Security IP cores. The design team really focused on providing tremendous efficiency to make embedded security integration much easier and straightforward. We are proud to propose universal, fast & small footprint solutions, supporting a lot of capabilities for a wide range of applications and technologies." says Philippe Lorent, Product Manager at Barco Silex.

Public Key cryptography is mainly used for digital signature and key exchange protocols. While symmetric cryptography like AES, requires large throughput and tricky features, asymmetric cryptography like RSA, is a very compute-intensive process that consumes a lot of CPU resources in security systems.

Software solutions running on embedded CPU are often too slow for applications with real-time requirements. The overhead generated on the CPU has an impact on performances that quickly becomes a penalty for the whole system. On the other hand, current hardware accelerators often consume a large part of the silicon and are not flexible enough to be used as stand-alone solutions.

It is to overcome these issues that Barco Silex introduced this BA414E Public Key Crypto Engine, a flexible, scalable and portable hardware accelerator IP.

The BA414E, based on a scalable, highly pipelined and optimized arithmetic unit, exploits efficiently the high potential of parallelism offered by hardware implementations. Such solutions provide the best trade-off between performance and area in any configuration. With the use of re-configurable elementary DSP blocks, the BA414E can be easily mapped to any existing FPGA technology as well as all ASIC processes.

Barco Silex
Rue du Bosquet 7
B-1348 Louvain la Neuve
www.barcodesignservices.com
www.barco.com/crypto



Press release

"With just less than 30k ASIC gates, the BA414E is the ideal solution for applications with strong constraints on cost & power." continues Philippe Lorent. "By just stretching the hardware, the same core is able to execute more than 5000 operations per second for 1024-bit CRT sign or decrypt."

The BA414E is a "Smart Engine", this means that it does not require any assistance from the main CPU to handle the complete Public Key processing. Based on a cost-effective μ -coded sequencer (coupled to a μ -DMA), the core is able to support a lot of complex operations and algorithms like RSA, CRT, DSA & ECDSA, including Pre- & post-processing.

"Selecting and integrating an IP Core remains a challenging process. I know that the BA414E Public Key Crypto Engine will solve recurrent IP problems. With its 100% CPU offload solution, it will simplify the integration of Public Key solutions. Best of all, it will keep silicon resources and power consumption at an extremely low level. Based on the same philosophy, Barco Silex will soon introduce the enhanced version of its AES hardware accelerator, the BA411E." says Thierry Pauwels, Marketing & Sales support for IP Business at Barco Silex.

With the announcement of this new Public Key Crypto Engine, Barco Silex emphasizes its continuous will to offer high-added value solutions and services to help its customers to build more secure designs while meeting stronger constraints of time, budget & power.

About Barco Silex

Barco Silex is a leader in contract engineering services, custom hardware and software development, as well as Intellectual Property (IP). Its high quality JPEG 2000 IP cores, developed since 2002, are optimized for all leading-edge FPGAs as well as for legacy platforms. Thanks to its continued stream of aggressive innovations, Barco Silex stays ahead of the competition. Barco Silex's history as a custom electronic design house (ASIC, FPGA, DSP, Board) specialized in video coding, cryptography, security and memory controllers goes back to 1991, offering the best guarantee for continuous support throughout the complete lifecycle of products.

About Barco

Barco, a global technology company, designs and develops visualization products for a variety of selected professional markets. Barco has its own facilities for Sales & Marketing, Customer Support, R&D and Manufacturing in Europe, North America and Asia Pacific. Barco (NYSE Euronext Brussels: BAR) is active in more than 90 countries with about 3,500 employees worldwide. Barco posted sales of 897 million euro in 2010.

© Copyright 2011 by Barco